1967

Modules of Quaternions and Their Related Quadratic Forms.

Charles Carter Waid
Louisiana State University and Agricultural & Mechanical College

MODULES OF QUATERNIONS AND THEIR RELATED QUADRATIC FORMS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Charles Carter Waid
B.S., New Mexico Institute of Mining and Technology, 1961
M.S., Louisiana State University, 1964
August, 1967

ACKNOWLEDGMENT

The author wishes to express his appreciation to Dr. Gordon Pall, under whose direction this dissertation was written, for his advice and encouragement.

TABLE OF CONTENTS

ABSTRACT

This thesis is concerned with modules and ideals of integral quaternions. The first two chapters are primarily concerned with developing the general properties of quaternion algebras and their integral subrings.

A simple definition of quaternion algebras is given in Chapter I, and their basic properties are derived. Using these properties, Pall's characterization of quaternion algebras in terms of ternary quadratic forms is obtained. The remainder of the chapter is devoted to proving various isomorphism theorems.

The notion of integrality is introduced in Chapter II, and the general properties of rings of integral quaternions over principal ideal domains are developed. The correspondence, first discovered by Pall, between classes of integral ternary forms and principal orders is derived. Using this, the following interesting decomposition theorem is proven:

> Every principal quaternion order Θ admits a decomposition $\Theta = R \oplus S \cdot \frac{x}{s}$ where R is a quadratic subring of Θ, S is a primitive ideal in R whose norm is s, and $x \in \Theta$.

In Chapter III, the maximal orders over the p-adic integers are studied. If $\Theta = \Theta(f)$ is a maximal local order, it is shown that $\Theta \cong M_2(Z_p)$ when $c_p(f) = 1$ and that Θ is a non-commutative valuation ring when $c_p(f) = -1$. Both of these rings are principal ideal rings and extensive use is made of this fact in proving locally the global theorems of Chapter IV. The crucial result is that if $\alpha, \beta \in \Theta$ and

$N\alpha \equiv N\beta \equiv (\alpha,\beta) \equiv 0 \bmod p$, then α and β are both contained in the same maximal right ideal or both contained in the same maximal left ideal.

Principal orders over the rational integers are studied by localizing to the p-adic case. The rules for going back and forth between the local and global cases are given, and a unique primary decomposition theorem for modules is proven. The good primes for an order Θ are defined to be those primes for which the local order Θ_p is maximal. The ideal theory for those ideals whose norms are products of good primes is developed, and the following theorem is proven:

> Let A be a primitive 4-dimensional submodule of $\Theta(f)$, $G_A = mF_A$ where m is the product of good primes and $\det F_A = \det F_\Theta$. Then there exists a unique triplet of integers (a,b,c) and unique right, two-sided, and left ideals, R, I, and L, respectively, such that
>
> (1) $A = R \cdot I \cdot L$
>
> (2) $m = abc$ with b the largest factor of m that is the product of primes for which $c_p(f) = -1$.
>
> (3) $n(R) = a$, $n(I) = b$, $n(L) = c$.

As an application of this theorem it is shown that if T is a 4×4 orthogonal matrix, that is, if $T'T = mI$, m a positive odd integer, then there exist matrices

$$M = \begin{bmatrix} x_0 & -x_1 & -x_2 & -x_3 \\ x_1 & x_0 & -x_3 & x_2 \\ x_2 & x_3 & x_0 & -x_1 \\ x_3 & x_2 & x_1 & x_0 \end{bmatrix}, \qquad N = \begin{bmatrix} y_0 & -y_1 & -y_2 & -y_3 \\ y_1 & y_0 & y_3 & -y_2 \\ y_2 & -y_3 & y_0 & y_1 \\ y_3 & y_2 & -y_1 & y_0 \end{bmatrix}$$

with $x_0^2 + x_1^2 + x_2^2 + x_3^2 = m_1$, $y_0^2 + y_1^2 + y_2^2 + y_3^2 = m_2$, $m = m_1 m_2$,

and a unit modular matrix U such that $T = MNU = NMU$.

CHAPTER I

QUATERNION ALGEBRAS

There are many different ways of defining a quaternion algebra. Since this thesis is primarily concerned with rings of integral quaternions and their ideals we shall define the algebra in a way that will allow the speedy development of the basic properties we need.

Let k be a field of characteristic $\neq 2$ and $\mathcal{A}$ a 4-dimensional vector space over k with basis ρ_0, ρ_1, ρ_2, ρ_3. Let $a, b \neq 0 \in k$ and define multiplication for the ρ_k by the following table.

	ρ_0	ρ_1	ρ_2	ρ_3
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3
ρ_1	ρ_1	a	ρ_3	$a\rho_2$
ρ_2	ρ_2	$-\rho_3$	b	$-b\rho_1$
ρ_3	ρ_3	$-a\rho_2$	$b\rho_1$	$-ab$

We extend the multiplication by linearity and obtain an associative algebra $\mathcal{A}$ called the quaternion algebra $(\frac{a,b}{k})$. As usual we will imbed k in $\mathcal{A}$ by identifying 1 and ρ_0.

Let $\alpha = a_0 + a_1\rho_1 + a_2\rho_2 + a_3\rho_3 \in \mathcal{A}$, $a_i \in k$.

We define the conjugate of α to be the quaternion

$$\bar{\alpha} = a_0 - a_1\rho_1 - a_2\rho_2 - a_3\rho_3 .$$

It is easily seen for $c \in k$, $\alpha, \beta \in \mathcal{A}$ that

$$\overline{c\,\alpha} = c\,\bar{\alpha} , \quad \overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta} , \quad \overline{\alpha\,\beta} = \bar{\beta}\,\bar{\alpha} .$$

We define the norm N and trace T of α by the equations

$$N\,\alpha = \alpha\,\bar{\alpha} , \qquad T\,\alpha = \alpha + \bar{\alpha} .$$

It follows that

$$N\,\alpha = a_0^2 - aa_1^2 - ba_2^2 + aba_3^2 , \quad T\alpha = T\,\bar{\alpha} .$$

For any $\alpha, \beta \in \mathcal{A}$, we have

$$N(\alpha\beta) = N\alpha \cdot N\beta , \quad T(\alpha + \beta) = T\alpha + T\beta .$$

A quaternion α is called pure if $T\alpha = 0$. Since

$0 = (\alpha - \alpha)(\alpha - \bar{\alpha}) = \alpha^2 - (T\alpha)\alpha + N\alpha$ we see that every quaternion is a root of a quadratic polynomial in $k[x]$. The following lemmas are easily verified [5;142][1].

---

[1] Pairs of Arabic numerals in brackets refer to correspondingly numbered references in the Selected Bibliography and page numbers, respectively. A single Arabic numeral in a bracket refers to the correspondingly numbered reference in the Selected Bibliography.

(1.1) Lemma. $\alpha \in \mathcal{A}$ is invertible if and only if $N\alpha \neq 0$. If this condition is satisfied, then $\alpha^{-1} = (N\alpha)^{-1}\bar{\alpha}$.

(1.2) Lemma. $\mathcal{A}$ is central simple.

(1.3) Lemma. If α and β are elements of an associative algebra $\mathfrak{J}$ over k such that $\alpha^2 = a$, $\beta^2 = b$, $\alpha\beta = -\beta\alpha$ with $a, b \neq 0 \in k$, then the subalgebra $\mathcal{B} = k + k\alpha + k\beta + k\alpha\beta$ is isomorphic to $(\frac{a,b}{k})$.

An important application of (1.3) is that $(\frac{1,-1}{k})$ is isomorphic to the algebra $M_2(k)$ of 2×2 matrices over k. For let e_{11}, e_{12}, e_{21}, e_{22} be the defining matrices of $M_2(k)$. Then $e_{11} + e_{22}$ is the identity matrix of $M_2(k)$. Now set $\alpha = e_{21} + e_{12}$ and $\beta = e_{21} - e_{12}$. Then $\alpha^2 = 1$, $\beta^2 = -1$, and $\alpha\beta = -\beta\alpha$.

If $\xi = x_0 + x_1\rho_1 + x_2\rho_2 + x_3\rho_3 \in \mathcal{A}$, we have seen that $N\xi = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$. If the x_i are considered as indeterminates over k, then $F(x_0, x_1, x_2, x_3) = N\xi$ is a quaternary quadratic form over k with non-zero square determinant. The form F is called the norm form of $\mathcal{A}$ for the basis $1, \rho_1, \rho_2, \rho_3$. If $\alpha, \beta \in \mathcal{A}$, then

$$(\alpha, \beta) = \alpha\bar{\beta} + \beta\bar{\alpha} = T(\alpha\bar{\beta})$$

is a symmetric bilinear form. It has the following useful properties.

(1.4) (i) $N\alpha = \frac{1}{2}(\alpha, \alpha)$, $\quad T\alpha = (1, \alpha)$

(ii) $(\alpha\beta, \alpha\gamma) = N\alpha \cdot (\beta, \gamma)$, $(\beta\alpha, \gamma\alpha) = N\alpha \cdot (\beta, \gamma)$

(iii) $(\alpha\beta, \gamma) = (\beta, \overline{\alpha}\,\gamma) = (\alpha, \gamma\,\overline{\beta})$.

Now consider an arbitrary basis $\lambda_0, \lambda_1, \lambda_2, \lambda_3$ for $\mathcal{A}$ over k and let $\xi = \Sigma\, x_i\lambda_i$. Then $G(x_0, x_1, x_2, x_3) = N\xi = \frac{1}{2}(\xi, \xi) = \frac{1}{2}(\Sigma\, x_i\lambda_i, \Sigma\, x_j\lambda_j)$ $= \sum_{i,j} \frac{1}{2}(\lambda_i, \lambda_j)x_i x_j$ is a quaternary quadratic form called the norm form for the basis $\lambda_0, \lambda_1, \lambda_2, \lambda_3$. Let $T = (t_{ij})$ be the 4×4 matrix taking the ρ basis onto the λ basis. That is, $\lambda_i = \sum_k \rho_k t_{ki}$. Then $(\lambda_i, \lambda_j) = (\sum_k \rho_k t_{ki}, \sum_m \rho_m t_{mj}) = \sum_{k,m} t_{ki}(\rho_k, \rho_m)t_{mj}$. Thus $G = F^T$ and $\det(G) = \det(T)^2 \det(F)$.

A basis $\theta_0 = 1, \theta_1, \theta_2, \theta_3$ for $\mathcal{A}$ over k with $\theta_1, \theta_2, \theta_3$ pure will be called a pure basis. We shall determine the multiplication table for such a basis. Since each of $\theta_1, \theta_2, \theta_3$ is pure, the matrix taking the ρ basis onto the θ basis is of the form

$$\begin{bmatrix} 1 & 0 \\ 0 & T \end{bmatrix}$$

where $T = (t_{ij})$ is a 3×3 matrix of non-zero determinant t. Moreover, the norm form for the θ basis is $G = x_0^2 + \sum_{i,j=1}^{3} \frac{1}{2}(\theta_i, \theta_j)x_i x_j$.

Let $\Delta_{ij} = \frac{1}{2}(\theta_i, \theta_j)$ and $\Delta = (\Delta_{ij})$. We have the equations

$$\Delta = T' \begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix} T \ , \qquad \det(\Delta) = (abt)^2.$$

Let $\partial = (\partial_{ij}) = (abt)^{-1}\mathrm{adj}(\Delta)$. Then $\mathrm{adj}(\partial) = \Delta$. We will denote the symmetric group on $\{1,2,3\}$ by S_3. If $\sigma \in S_3$ then $|\sigma| = +1$ or -1 according as σ is an even or odd permutation.

(1.5) Lemma. $(1, \rho_i \rho_j \rho_k) =$

$-|\sigma|ab$ if $\sigma = (i,j,k) \in S_3$

0 if two of i,j,k are equal.

Proof: An easy verification.

(1.6) Lemma. If $\sigma = (i,j,k) \in S_3$, then $(1,\theta_i\theta_j\theta_k) = -|\sigma|abt$.

Proof: By repeated application of property (1.4.iii) of the inner product we have $(1,\theta_i\theta_j\theta_k) = |\sigma|(1,\theta_1\theta_2\theta_3)$. But $(1,\theta_1\theta_2\theta_3) =$

$$(1, \sum_i \rho_i t_{i1} \cdot \sum_j \rho_j t_{j2} \cdot \sum_k \rho_k t_{k3}) = \sum_{i,j,k} (1, \rho_i \rho_j \rho_k) t_{i1} t_{i2} t_{i3}$$

$$= -ab \sum_{\sigma \in S_3} |\sigma| t_{\sigma(1)1} t_{\sigma(2)2} t_{\sigma(3)3} = -abt.$$

Q.E.D.

Using (1.4) and (1.6), we have, for $(i,j,k) \in S_3$, that

$$
\begin{aligned}
&(1,\theta_i\theta_j) = (\overline{\theta}_i,\theta_j) = -(\theta_i,\theta_j) = -2\Delta_{ij} \\
&(\theta_i,\theta_i\theta_j) = N\theta_i\cdot(1,\theta_j) = 0 \\
&(\theta_j,\theta_i\theta_j) = N\theta_j\cdot(1,\theta_i) = 0 \\
&(\theta_k,\theta_i\theta_j) = (1,\theta_i\theta_j\overline{\theta}_k) = -(1,\theta_i\theta_j\theta_k) = |\sigma|abt
\end{aligned}
\tag{1.7}
$$

For $\sigma = (i,j,k)$, $P(\sigma)$ will denote the 3 x 3 matrix whose first, second, and third rows are the ith, jth, and kth rows, respectively, of the 3 x 3 identity matrix. Note that $P(\sigma)^{-1} = P(\sigma)'$. We can now find the multiplication table for the pure basis $1, \theta_1, \theta_2, \theta_3$. We have $\theta_i\theta_j = x_0 + x_1\theta_1 + x_2\theta_2 + x_3\theta_3$ with $x_i \in k$. Thus

$$
\begin{aligned}
&(1,\theta_i\theta_j) = 2x_0 \\
&(\theta_i,\theta_i\theta_j) = x_1(\theta_i,\theta_1) + x_2(\theta_i,\theta_2) + x_3(\theta_i,\theta_3) \\
&(\theta_j,\theta_i\theta_j) = x_1(\theta_j,\theta_1) + x_2(\theta_j,\theta_2) + x_3(\theta_j,\theta_3) \\
&(\theta_k,\theta_i\theta_j) = x_1(\theta_k,\theta_1) + x_2(\theta_k,\theta_2) + x_3(\theta_k,\theta_3)
\end{aligned}
\tag{1.8}
$$

Equating (1.7) and (1.8) and putting in matrix form we have

$$x_0 = -\Delta_{ij}$$

$$(|\sigma|abt)\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = P(\sigma)\cdot\Delta\cdot\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} .$$

Solving for the x_i we have

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = (|\sigma| abt)\cdot \Delta^{-1} P(\sigma)^{-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = |\sigma| \partial \cdot P(\sigma)' \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} .$$

Thus the multiplication table for the θ basis is given by

$$\theta_i^2 = -\Delta_{ii}$$

(1.9)

$$\theta_i\theta_j = -\Delta_{ij} + |\sigma|(\partial_{1k}\theta_1 + \partial_{2k}\theta_2 + \partial_{3k}\theta_3) \text{ for } \sigma = (i,j,k) \in S_3.$$

Let f be a non-singular ternary form over k with matrix ∂ and let $\Delta = \text{adj}(\partial)$. $\mathcal{A}(f)$ will denote the 4-dimensional algebra over k with basis $\theta_0 = 1, \theta_1, \theta_2, \theta_3$ satisfying the multiplication table given by (1.9).

(1.10) Theorem. Every quaternion algebra is an $\mathcal{A}(f)$ algebra and conversely every $\mathcal{A}(f)$ algebra is a quaternion algebra. Moreover, $F_{\mathcal{A}} = x_0^2 + \text{adj } f(x_1, x_2, x_3)$.

Proof: Let $f = -bx^2 - ay^2 + z^2$, $a,b \neq 0 \in k$. Clearly $\mathcal{A}(f) \simeq (\frac{a,b}{k})$. Now let f, ∂, Δ be given. By using the fact that $\det(\Delta) = \det(\partial)^2$ is a non-zero square, it is easy to see that there exist a, $b \neq 0 \in k$ and a 3 × 3 matrix T of determinant $t \neq 0$ such that

$$\Delta = (\pm T') \begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix} (\pm T) .$$

Thus $\det(\partial) = \pm abt$. We choose T or -T so that $\det(\partial) = abt$. Thus there exists a pure basis 1, $\theta = \rho T$ of $(\frac{a,b}{k})$ which has the same multiplication table as the basis for $\mathcal{A}(f)$. Therefore $\mathcal{A}(f) \simeq (\frac{a,b}{k})$. Clearly $F_{\mathcal{A}} = x_0^2 + \text{adj } f(x_1, x_2, x_3)$.

Q.E.D.

(1.11) Theorem. If $\text{adj}(f^*) = \text{adj}(f)^T$ and if $\theta = (\theta_1, \theta_2, \theta_3)$ and $\theta^* = (\theta_1^*, \theta_2^*, \theta_3^*)$, then there is a sign $e = \pm 1$ such that the map $\mathcal{A}(f^*) \xrightarrow{\tau} \mathcal{A}(f)$ defined by $\tau(1) = 1$, $\tau(\theta^*) = \theta(eT)$ is an isomorphism.

Proof: By (1.10) there exist $a, b \neq 0 \in k$ and an isomorphism $\mathcal{A}(f) \xrightarrow{\mu} (\frac{a,b}{k})$ defined by $\mu(1) = 1$, $\mu(\theta) = \rho U$ for U a 3 x 3 matrix such that

$$\Delta = U' \begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix} U.$$

Thus $\Delta^* = T' \Delta T = T'U' \begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix} UT$ and hence

by (1.10) there exists a sign $e = \pm 1$ such that the map $\mathcal{A}(f^*) \xrightarrow{\eta} (\frac{a,b}{k})$ defined by $\eta(1) = 1$, $\eta(\theta^*) = \rho(eUT)$ is an isomorphism. Let $\tau = \mu^{-1}\eta$. Then $\tau(1) = 1$ and $\tau(\theta^*) = \mu^{-1}(\rho(eUT)) = \theta U^{-1} \cdot U \cdot (eT) = \theta \cdot eT$.

Q.E.D.

(1.12) Theorem. If $f^* = f^U$ and $T' = \text{adj } U$, then the map $\mathcal{A}(f^*) \xrightarrow{\tau} \mathcal{A}(f)$ defined by $\tau(1) = 1$, $\tau(\theta^*) = \theta T$ is an isomorphism.

Proof: We may assume $\mathcal{A}(f) = (\frac{a,b}{k})$ and thus $\theta = \rho S$ for some S of determinant $s \neq 0$. Then we must have $\partial = (abs)^{-1}\text{adj}(\Delta)$ and thus $\det(\partial) = (abs)^{-3}(abs)^4 = abs$. Let $\theta' = \theta T = \rho ST$. Then again $\det(\partial') = absu^2$ where $u = \det(U)$. But $\det(\partial^*) = u^2\det(\partial) = absu^2$ and $\Delta^* = \text{adj}(\partial^*) = \text{adj } U \cdot \Delta \cdot \text{adj } U' = T'\Delta T = \Delta' = \text{adj}(\partial')$. Thus $\partial^* = \partial'$ and τ is an isomorphism.

Q.E.D.

CHAPTER II

ORDERS, IDEALS, AND MODULES

Let R be a principal ideal domain whose quotient field is k and let $\mathcal{A}$ be a quaternion algebra over k. A quaternion $\alpha \in \mathcal{A}$ will be called R-integral or simply integral if $T\alpha$, $N\alpha \in R$. A subset Θ of $\mathcal{A}$ will be called an R-order or simply an order if Θ satisfies the following axioms.

(2.1) (i) Θ is a ring.

(ii) If $\alpha \in \mathcal{A}$, then there exists $m \neq 0 \in R$ such that $m\alpha \in \Theta$.

(iii) Θ is a finitely generated R module.

By (ii), Θ contains a basis for $\mathcal{A}$ over k, and (iii) implies that is a free R-module since R is a principal ideal domain. Thus Θ is a 4-dimensional R-module. If $\omega_0, \omega_1, \omega_2, \omega_3$ is an R-basis for the order Θ, we write $\Theta = R\omega_0 + R\omega_1 + R\omega_2 + R\omega_3 = R[\omega_0,\omega_1,\omega_2,\omega_3]$ or simply $\Theta = [\omega_0,\omega_1,\omega_2,\omega_3]$.

(2.2) Theorem. An order $\Theta = [\omega_0,\omega_1,\omega_2,\omega_3]$ consists entirely of integral quaternions.

Proof: We can choose an R basis for Θ with $\omega_0 \in k$. But $\omega_0 \cdot \omega_0 \in \Theta$ and hence $\omega_0 \in R$. Moreover, $\omega_i^2 = -N\omega_i + (T\omega_i)\omega_i \in \Theta$ and thus $T\omega_i$, $N\omega_i \in R$. Therefore, $\overline{\omega}_i\omega_j = (T\omega_i - \omega_i)\omega_j \in \Theta$ and hence $(\omega_i, \omega_j) = T(\overline{\omega}_i\omega_j) \in R$. Now let $\xi = \Sigma x_i\omega_i \in \Theta$, $x_i \in R$. Then

$$T\,\xi = \Sigma x_i \cdot T\omega_i \in R, \text{ and}$$

$$N\,\xi = \tfrac{1}{2}(\xi, \xi) = \tfrac{1}{2}\Sigma(\omega_i, \omega_j)x_i x_j = \Sigma(N\omega_i)x_i^2 + \sum_{i<j}(\omega_i, \omega_j)x_i x_j \in R.$$

Q.E.D.

(2.3) Theorem. If $\Theta \subset \mathcal{A}$ satisfying (i) and (ii) of (2.1) and if also

(iii') Every member of Θ is integral,

then Θ is an order.

Proof: if $\alpha, \beta \in \Theta$ then $\alpha\beta \in \Theta$ and hence $T(\alpha\beta) \in R$. But $T(\alpha\beta) = (1, \alpha\beta) = (\overline{\alpha}, \beta) = (T\alpha - \alpha, \beta) = T\alpha \cdot T\beta - (\alpha, \beta)$. Therefore, since $T\alpha$, $T\beta \in R$ we have $(\alpha, \beta) \in R$. By (2.1.ii), there exists a basis $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \Theta$ for $\mathcal{A}$ over k. Thus if $\xi \in \Theta$, there exist $x_i \in k$ such that $\xi = \Sigma x_i\alpha_i$. Moreover, $r_j = (\xi, \alpha_j) = \sum_i x_i(\alpha_i, \alpha_j) \in R$. If we let A be the matrix $((\alpha_i, \alpha_j))$, then solving for the x_i's gives

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = A^{-1} \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} = \frac{\text{adj } A}{\det A} \cdot \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} .$$

Since A has coefficients in R, adj A has coefficients in R and det A is in R. Thus, $\Theta \subset (\det A)^{-1} \cdot R[\alpha_0, \alpha_1, \alpha_2, \alpha_3]$ and therefore is a finitely generated R-module.

Q.E.D.

An order containing the identity will be called a <u>principal order</u>. If Θ is a principal order and $A \subset \mathcal{A}$ such that

(2.4)
- (i) A is closed under addition,
- (ii) $A\Theta \subset A$,
- (iii) There exists an $m \neq 0 \in R$ such that $mA \subset \Theta$,

then A is called a <u>fractional right ideal</u> in Θ. <u>Fractional left</u> and <u>two-sided ideals</u> in Θ are defined analogously.

If A is a fractional ideal in Θ and if $A \subset \Theta$, then A is called an <u>integral ideal</u> or simply an <u>ideal</u> in Θ. If A is a fractional ideal in Θ, then $mA \subset \Theta$ for some $m \neq 0 \in R$. Thus mA, and therefore A, is a free R-module. We will be interested primarily in 4-dimensional R-modules. We will often use the notation [A), (A], (A) for right, left, and two-sided ideals, respectively.

Now let $\Theta = [\omega_0, \omega_1, \omega_2, \omega_3]$ be a principal order and $A = [\alpha_0, \alpha_1, \alpha_2, \alpha_3]$ be a 4-dimensional R-module contained in Θ. In the following, we will define the symbols l(A), N(A), and n(A) to be certain non-zero ideals of R; in the special case R = Z (the rational integers) the symbol will be taken as denoting the positive integer generating the ideal, and in the case $R = Z_p$ (the p-adic integers), the power of p generating the ideal.

(2.5) Let $\underline{l(A) = R \cap A}$. Note that A has an R basis α_0, α_1, α_2, α_3 with $\alpha_0 \in R$ and thus, $l(A) = (\alpha_0)$. Let $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ and $\omega = (\omega_0, \omega_1, \omega_2, \omega_3)$. There is a 4×4 matrix T with coefficients in R such that $\alpha = \omega T$. Since A is 4-dimensional $\det T \neq 0$.

(2.6) Let $\underline{N(A) = (\det T) \cdot R}$. N(A) is called the norm of the module A. In the case R is Z or Z_p it is well known [4;54] that N(A) is the number of residue classes in the difference module Θ/A.

Solving $\alpha = \omega T$ for ω we obtain $\omega = \alpha \cdot \frac{\text{adj } T}{\det T}$. We now cancel all factors of det T that divide all of the coefficients of adj T and obtain $\omega = \alpha \cdot \frac{S}{h}$ where S is a 4×4 matrix with coefficients in R, $h \in R$, and no divisor of h divides all the coefficients of S. In fact, S is primitive as can be seen by the equation $T \cdot \text{adj } T = (\det T) \cdot I$, which gives $T \cdot S = h \cdot I$.

(2.7) Let $\underline{n(A) = h \cdot R}$. n(A) is called the reduced norm of A. n(A) is the maximal ideal (b) in R for which $(b) \cdot \Theta \subset A$. For if the prime ideal

(p) divides n(A), then $p \mid h$ and there is a coefficient s_{ij} of S for which $p \nmid s_{ij}$. Now let $p^n \| h$ and suppose $(b)\cdot\Theta \subset A$. Then $bw_j \in A$ and hence $\frac{bs_{ij}}{h} \in R$. Thus $p^n \mid b$ and therefore $n(A) \supset (b)$. It is clear that $l(A)$, $N(A)$, and $n(A)$ are independent of choice of basis for A and Θ and that $l(A) \supset n(A) \supset N(A)$.

Let $\xi = \Sigma x_i \alpha_i \in A$. We define the quadratic form G_A by the equation $G_A = N\xi$. G_A has coefficients in R and can be expressed as the product of an element m of R and a primitive quadratic form F_A. Thus, $G_A = mF_A$. G_A and F_A are determined up to an R-unit modular transformation. For any choice of basis for A we call G_A the <u>norm form</u> of A and F_A the <u>primitive part of the norm form</u> of A. If T is the matrix carrying Θ onto A then $G_A = G_\Theta^T$ and thus $\det G_A = (\det T)^2 \cdot \det G_\Theta = N(A)^2 \cdot \det G_\Theta$. Clearly, $G_\Theta = F_\Theta$ and if $\det G_A$ is a unit multiple of $\det F_\Theta$ then $A = \Theta$.

(2.8) A subset A of Θ is said to be <u>primitive</u> if whenever $A \subset b\cdot\Theta$ with $b \in R$, then b is a unit of R.

(2.9) <u>Theorem</u>. If $A = [\alpha)$ is a primitive principal right ideal in Θ, then

(i) α is primitive,

(ii) $(N\alpha)\cdot R = l(A) = n(A)$,

(iii) $N(A) = n(A)^2$.

Proof: (i) is clear. Thus $\overline{\alpha}$ is primitive. It is also clear that $l(A) = n(A)$. Now suppose $n(A) = mR$. Then there is a $\beta \in \Theta$ such that $\alpha\beta = m$. Hence, $(N\alpha)\cdot\beta = \overline{\alpha}\,\alpha\beta = m\,\overline{\alpha}$ and $\beta = \frac{m}{N\alpha}\cdot\overline{\alpha}$. Since $\overline{\alpha}$ is primitive we have $N\alpha \mid m$. But $N\alpha = \alpha\,\overline{\alpha} \in A$ and thus $N\alpha\cdot R = n(A)$. It is clear that $G_A = (N\alpha)\cdot F_\Theta$. Thus $\det G_A = (N\alpha)^4\cdot\det F_\Theta = N(A)^2\cdot\det F_\Theta$. Therefore, $N(A) = (N\alpha)^2\cdot R = n(A)^2$.

Q.E.D.

An order Θ of $\mathcal{A}$ is said to be maximal if it is not properly contained in any order of $\mathcal{A}$. If $\Theta(f')$ properly contains $\Theta(f)$, then the transformation carrying $\Theta(f')$ onto $\Theta(f)$ has non-unit determinant. Thus, since $4\cdot\det f$ is in R if f has coefficients in R, we have $(4\cdot\det f')\cdot R$ properly contains $(4\cdot\det f)\cdot R$. It follows that every order is contained in a maximal order. A maximal order must be principal since $R + \Theta$ is an order if Θ is an order.

We will now study principal orders more closely. The first thing we shall do is develop the multiplication table for a principal order and in doing so derive Pall's characterization of principal orders [6;285] which will be used throughout this thesis. Let $\Theta = [1,\omega_1,\omega_2,\omega_3]$ be a principal order and for convenience let $b_i = T\omega_i$ and $c_{ij} = \frac{1}{2}(\omega_i,\omega_j)$. Then $F_\Theta = x_0^2 + \Sigma\, b_i x_0 x_i + \Sigma\, c_{ij} x_i x_j$. If $\theta_i = \omega_i - \frac{1}{2}b_i$, then $1, \theta_1, \theta_2, \theta_3$ is a pure basis for $\mathcal{A}$ over k with multiplication table given by (1.9). Moreover, $\Delta_{ij} = \frac{1}{2}(\theta_i,\theta_j) = c_{ij} - \frac{b_i b_j}{4}$. Thus,

$$\omega_i^2 = -(\Delta_{ii} + \tfrac{1}{4} b_i^2) + b_i \omega_i$$

and, for $\sigma = (i,j,k) \in S_3$,

(2.10)
$$\omega_i \omega_j = -(\Delta_{ij} + \tfrac{1}{4} b_i b_j + \tfrac{1}{2}|\sigma| \sum_m \partial_{mk} b_m)$$
$$+ (|\sigma|\partial_{ik} + \tfrac{b_j}{2})\omega_i + (|\sigma|\partial_{jk} + \tfrac{b_i}{2})\omega_j + |\sigma|\partial_{kk}\omega_k.$$

Since the coefficients of ω_1, ω_2, and ω_3 in the product $\omega_i \omega_j$ must lie in R, we have ∂_{kk}, $2\partial_{ij} \in R$ and thus ∂ is the matrix of a ternary quadratic form with coefficients in R. Furthermore, $2\partial_{ik} \equiv b_j \bmod 2$. Since $\Delta_{ij} = \partial_{ik}\partial_{jk} - \partial_{ij}\partial_{kk}$ we have $\Delta_{ij} + \tfrac{1}{4} b_i b_j + \tfrac{1}{2}|\sigma| \sum_m \partial_{mk} b_m$ $= (\partial_{ik} + \tfrac{1}{2}|\sigma| b_j)(\partial_{jk} + \tfrac{1}{2}|\sigma| b_i) + \partial_{kk}(\tfrac{1}{2}|\sigma| b_k - \partial_{ij})$ which is always integral. If we let $\omega_i' = \tfrac{1}{2} b_i' + \theta_i$ with $b_i' \equiv b_i \bmod 2$, then it is clear that $[1, \omega_1', \omega_2', \omega_3'] = [1, \omega_1, \omega_2, \omega_3]$. Thus we have proven

(2.11) Theorem. Let f be a ternary form with coefficients in R and matrix ∂. Choose $e_i = 0$ or 1 according as $2\partial_{jk} \equiv 0$ or 1 mod 2. Let $\omega_i = \tfrac{1}{2} e_i + \theta_i$. Then $[1, \omega_1, \omega_2, \omega_3]$ is a principal order. Moreover, every principal order can be obtained in such a manner.

We shall denote the principal order of (2.11) by $\Theta(f)$.

(2.12) Theorem. Let f and f^* be non-singular ternary forms with coefficients in R and T be a 3 x 3 matrix with coefficients in R such that adj f^* = (adj f)^T. If $\Theta(f) = [1,\omega_1,\omega_2,\omega_3]$ and $\Theta(f^*) = [1,\omega_1^*,\omega_2^*,\omega_3^*]$, then $\Theta(f^*) \simeq [1,\omega T]$ where $\omega = (\omega_1,\omega_2,\omega_3)$.

Proof: Let $\theta_i = \omega_i - \frac{1}{2}e_i$, $\theta_i^* = \omega_i^* - \frac{1}{2}e_i^*$, $\theta = (\theta_1,\theta_2,\theta_3)$, $\theta^* = (\theta_1^*,\theta_2^*,\theta_3^*)$, $\epsilon = (e_1,e_2,e_3)$, $\epsilon^* = (e_1^*,e_2^*,e_3^*)$, and $\omega^* = (\omega_1^*,\omega_2^*,\omega^*)$. Then we have $\omega = \frac{1}{2}\epsilon + \theta$ and $\omega^* = \frac{1}{2}\epsilon^* + \theta^*$. Moreover, $[1,\omega T] = [1,\omega(-T)]$ so we may assume the map $\mathcal{A}(f^*) \xrightarrow{\tau} \mathcal{A}(f)$ defined by $\tau(1) = 1$, $\tau(\theta^*) = \theta T$ is an isomorphism. Thus $\tau(\omega^*) = \tau(\frac{1}{2}\epsilon^* + \theta^*) = \frac{1}{2}\epsilon^* + \theta T = \omega T + \frac{1}{2}(\epsilon^* - \epsilon T)$. Hence, $[1,\tau(\omega^*)] = [1,\omega T]$ if and only if $\epsilon^* \equiv \epsilon T \bmod 2$. However, we know that

$$F_\Theta = x_0^2 + \Sigma e_i x_0 x_i + \Sigma c_{ij} x_i x_j \quad \text{and} \quad F_{\Theta^*} = x_0^2 + \Sigma e_i^* x_0 x_i + \Sigma c_{ij}^* x_i x_j$$

have coefficients in R, and that $4\Delta = 4(c_{ij}) - \epsilon'\epsilon$ and $4\Delta^* = 4(c_{ij}^*) - \epsilon^{*'}\epsilon^*$. Hence, $\epsilon^{*'}\epsilon^* \equiv 4\Delta^* \equiv T'4\Delta T \equiv T'\epsilon'\epsilon T \bmod 2$. It follows that $\epsilon^* \equiv \epsilon T \bmod 2$ and thus that $\Theta(f^*) \simeq [1,\omega T]$.

Q.E.D.

(2.13) Corollary. If the determinant of T is a unit in R, then $\Theta(f^*) \simeq \Theta(f)$. In particular, if U is a 3 x 3 unit modular matrix over R, then $\Theta(f) \simeq \Theta(f^U)$.

We have an interesting decomposition theorem for principal orders.

(2.14) Theorem. There is a basis $1, \omega_1, \omega_2, \omega_3$ for $\Theta(f)$ such that $\Theta(f) = [1,\omega_1] \oplus [\partial_{33},\omega_1]\frac{\omega_2}{\partial_{33}}$ where $[\partial_{33},\omega_1]$ is an integral ideal of the quadratic ring $[1,\omega_1]$.

Proof: Let $\omega_1 = -\partial_{23} + \theta_1$, $\omega_2 = -\partial_{13} + \theta_2$, $\omega_3 = \partial_{12} + \theta_3$. Then $\Theta(f)$ $= [1,\omega_1,\omega_2,\omega_3]$. But

$$\omega_1\omega_2 = \partial_{13}\partial_{23} - \partial_{13}\theta_1 - \partial_{23}\theta_2 - \Delta_{12} + \partial_{13}\theta_1 + \partial_{23}\theta_2 + \partial_{33}\theta_3$$

$$= \partial_{13}\partial_{23} - (\partial_{13}\partial_{23} - \partial_{12}\partial_{33}) + \partial_{33}\theta_3$$

$$= \partial_{33}\omega_3.$$

Thus $\Theta(f) = [1,\omega_1] \oplus [\partial_{33},\omega_1]\frac{\omega_2}{\partial_{33}}$. For $[\partial_{33},\omega_1]$ to be an ideal in $[1,\omega_1]$ it is necessary and sufficient that $\partial_{33} \mid N(\omega_1)$. But

$$N(\omega_1) = \tfrac{1}{2}(-\partial_{23} + \theta_1 - \partial_{23} + \theta_1) = \partial_{23}^2 + \Delta_{11}$$

$$= \partial_{23}^2 + (\partial_{22}\partial_{33} - \partial_{23}^2)$$

$$= \partial_{22}\partial_{33}.$$

Q.E.D.

—

CHAPTER III

THE LOCAL CASE

In the following $\mathbb{Q}$ will denote the rational numbers, Z the rational integers, and p a rational prime. $\mathbb{Q}_p$ will denote the p-adic completion of the rationals, Z_p the p-adic integers and $\mathcal{A} = \mathcal{A}(f)$ a quaternion algebra over $\mathbb{Q}_p$. We will study the theory of maximal Z_p-orders in $\mathcal{A}$.

(3.1) Theorem. Let $c_p(f)$ denote the Hasse symbol. If $c_p(f) = c_p(g)$, then $\mathcal{A}(f) \sim \mathcal{A}(g)$.

Proof: It is easily shown that $c_p(f) = c_p(\text{adj } f)$. Now suppose $c_p(f) = c_p(g)$. Then $c_p(\text{adj } f) = c_p(\text{adj } g)$ and moreover the the determinants of adj f and adj g are squares. Thus adj f and adj g are equivalent over $\mathbb{Q}_p$. Therefore, by (1.11), $\mathcal{A}(f) \sim \mathcal{A}(g)$. We must therefore separate the study of the local algebra into two cases according as $c_p(f) = -1$ or $c_p(f) = +1$.

A. The case $c_p(f) = -1$.

(3.2) Theorem. $\mathcal{A}(f)$ is a skew field.

Proof: The norm form for $\mathcal{A}(f)$ is $F_{\mathcal{A}} = x_0^2 + \text{adj } f$. But

$c_p(F_{\mathcal{A}}) = c_p(\text{adj } f) = c_p(f) = -1$ and $\det F_{\mathcal{A}}$ is a square. Hence, $F_{\mathcal{A}}$ does not represent zero in Q_p. This means that every non-zero element of $\mathcal{A}$ has a non-zero norm and therefore has an inverse.

Q.E.D.

(3.3) Let $\Phi = px^2 - \varphi(y,z)$ where

$$\varphi(y,z) = \begin{cases} -\nu y^2 + z^2 & \text{for } p \text{ odd with } \nu \text{ a fixed quadratic non-residue of } p \\ y^2 - yz + z^2 & \text{for } p = 2. \end{cases}$$

Φ is an integral form and $c_p(\Phi) = -1$. Hence, $\Theta = \Theta(\Phi) = Z_p[1, \omega_1, \omega_2, \omega_3]$ is a principal order of $\mathcal{A}$.

(3.4) Theorem. Θ is the unique maximal order of $\mathcal{A}$. Furthermore, $\alpha \in \mathcal{A}$ is integral if and only if $N\alpha \in Z_p$.

Proof: For p odd, $e_1 = e_2 = e_3 = 0$ and $\omega_i = \theta_i$. Thus, $F_\Theta = x_0^2 + \text{adj } \Phi = x_0^2 - \nu x_1^2 - p(x_2^2 - \nu x_3^2)$. For $p = 2$, $e_1 = 1$, $e_2 = e_3 = 0$ and therefore $\omega_1 = \frac{1}{2} + \theta_1$, $\omega_2 = \theta_2$, $\omega_3 = \theta_3$. Thus, $F_\Theta = x_0^2 + x_0x_1 + \frac{1}{4}x_1^2 + \text{adj } \Phi = x_0^2 + x_0x_1 + x_1^2 - 2(x_2^2 + x_2x_3 + x_3^2)$. Combining these two cases, we have $F_\Theta = \text{adj } \varphi(x_0, x_1) - p \cdot \text{adj } \varphi(x_2, x_3)$.

Notice that if $\text{adj } \varphi(x,y) \equiv 0 \bmod p$ for some $x, y \in Z_p$, then $x \equiv y \equiv 0 \bmod p$. Now let $\xi = x_0 + \sum x_i \omega_i \in \mathcal{A}$, $x_i \in Q_p$, and suppose $N\xi = h \neq 0 \in Z_p$. Pick $s \geq 0$ such that $y_i = p^s x_i$ is a p-adic integer

for each i and y_j is a p-adic unit for some j. Let $\eta = y_0 + \Sigma y_i\omega_i$ $= p^s\xi$. Then $N\eta = \text{adj}\ (y_0,y_1) - p\cdot\text{adj}\ (y_2,y_3) = p^{2s}h$. If $s > 0$, we have adj $\varphi(y_0,y_1) \equiv 0 \bmod p$ and, thus, $y_0 = py_0'$, $y_1 = py_1'$. Hence, $N\eta = p^2\cdot \text{adj}\ \varphi(y_0',y_1') - p\ \text{adj}\ \varphi' y_2,y_3) = p^{2s}h$, $s > 0$. It follows that adj $\varphi(y_2,y_3) \equiv 0 \bmod p$ and again $y_2 = py_2'$, $y_3 = py_3'$. This contradicts the assumption that one of the y_j is a unit. Therefore, $s = 0$ and each $x_i \in Z_p$. Thus, $\xi \in \Theta$ and, hence, is integral. It follows immediately that Θ is the unique maximal order of $\mathcal{A}$.

Q.E.D.

Now let $\pi = \omega_2$ and V be the p-adic valuation on Q_p. We see that $\pi^2 = p$ and that π is irreducible.

(3.5) Theorem. If $\alpha \neq 0 \in \mathcal{A}$, then $\alpha = \epsilon\pi^n = \pi^n\epsilon'$ for some integers n and some ϵ, $\epsilon' \in \mathcal{A}$ with $N\epsilon$ and $N\epsilon'$ p-adic units. Moreover,

(i) $\Theta = \{\alpha \in \mathcal{A} \mid V(N\alpha) \geq 0\}$

(ii) $U = \{\alpha \in \mathcal{A} \mid V(N\alpha) = 0\}$ is the set of units of Θ.

(iii) $P = \{\alpha \in \mathcal{A} \mid V(N\alpha) > 0\}$ is the unique maximal two-sided ideal in Θ.

The proof is obvious.

(3.6) Theorem. $P = \pi\cdot\Theta = (\pi)$, and the fractional ideals in Θ are two-sided and are the integral powers of (π).

Again the proof is easy.

(3.7) Theorem. (π) is the only proper primitive ideal in Θ and is 2-dimensional mod p.

Proof: It is clear that (π) is the only proper primitive ideal since $\pi^2 = p$. Also π, $\pi\omega_1$, $\pi\omega_2$, $\pi\omega_3$ is a Z_p basis for (π). By using the multiplication tables we have, both for $p = 2$ and p odd, that $\pi = \omega_2$, $\pi\omega_1 = \omega_3$, $\pi\omega_2 = p$, $\pi\omega_3 = p\omega_1$. Thus $(\pi) = [p, p\omega_1, \omega_2, \omega_3]$ and is clearly 2-dimensional mod p.

Q.E.D.

(3.8) Theorem. If A is a 4-dimensional submodule of Θ such that $G_A = p^h F_A$, where $\det F_A$ is a unit multiple of $\det F_\Theta$, then $A = (\pi^h)$.

Proof: Since the norm of every element of A is divisible by p^h it is clear that every element of A is divisible by π^h. Thus $A = \pi^h B$ and $G_B = F_A$. But $\det G_B = N(B)^2 \cdot \det F_\Theta$. Thus N(B) is a p-adic unit and $B = \Theta$. Therefore $A = (\pi^h)$.

Q.E.D.

B. The case, $c_p(f) = +1$.

(3.9) Theorem. $\mathcal{A}(f) \simeq M_2(Q_p)$.

Proof: Let $g = x^2 - y^2 + z^2$. $c_p(g) = +1$ and therefore $\mathcal{A}(f) \simeq \mathcal{A}(g) = \left(\frac{1,-1}{Q_p}\right) \simeq M_2(Q_p)$.

Q.E.D.

(3.10) Let $\Theta = M_2(Z_p)$.

(3.11) Theorem. Θ is a maximal order of of $\mathcal{A}$.

Proof: (Hasse) Suppose Θ^* is an order containing Θ and let $\alpha = \Sigma a_{ij}e_{ij} \in \Theta^*$, $a_{ij} \in Q_p$. Then for any i and j we have $a_{ij}e_{kk} = e_{ki}\alpha \cdot e_{jk} \in \Theta^*$ and, thus, $a_{ij}(e_{11} + e_{22}) = a_{ij} \in \Theta^* \cap Q_p = Z_p$. Thus $\alpha \in \Theta$.

Q.E.D.

(3.12) Lemma. Let R be a principal ideal ring, I_r the lattice of right ideals in $M_n(R)$, I_ℓ the lattice of left ideals in $M_n(R)$, and S the lattice of submodules of $\overset{n}{\underset{1}{\oplus}} R$. Define the mappings $I_r \xrightarrow{\rho} S$ and $I_\ell \xrightarrow{\lambda} S$ by letting $\rho(A)$ be the set of all vectors $(x_1,\ldots,x_n)$ occurring as a column of some matrix α in A and by letting $\lambda(B)$ be the set of all vectors $(x_1,\ldots,x_n)$ occurring as a row of some matrix β in B. Then

(i) ρ and λ are lattice isomorphisms,

(ii) the ideals in $M_n(R)$ are principal

(iii) the two-sided ideals of $M_2(R)$ are of the form $r \cdot M_n(R)$ with $r \in R$.

The proof is well known [3;]. However, the construction of a

generator of an ideal A is of interest. $\rho(A)$ or $\lambda(A)$ is a free R module since R is a principal ideal ring and hence has an R basis, say $x_1,\ldots,x_k$, $k \leq n$ with $x_i = (x_{1i},\ldots,x_{ni})$. Now let

$$\alpha = \begin{bmatrix} x_{11} & \cdots & x_{1k} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ x_{n1} & \cdots & x_{nk} & 0 & \cdots & 0 \end{bmatrix}$$

with enough columns of zeros so that α is an $n \times n$ matrix. If A is a right ideal then $A = [\alpha)$. If A is a left ideal, then $A = (\alpha']$, where α' is the transpose of α. The ideals in $M_2(Z_p)$ we are considering in this thesis are all 4-dimensional and therefore are generated by matrices with non-zero determinant. The submodules of $Z_p \oplus Z_p$ corresponding to these ideals are 2-dimensional.

(3.13) Theorem. Let $\alpha \in \mathcal{A}$ with $N\alpha \neq 0$. Then $\alpha^{-1}\Theta\,\alpha$ is a maximal order of $\mathcal{A}$ and every maximal order is one of these. All maximal orders have the same norm form F_Θ.

Proof: (Hasse) It is clear that $\alpha^{-1}\Theta\,\alpha$ is a maximal order of $\mathcal{A}$ and has the same norm form as Θ. Now let Θ^* be a maximal order of $\mathcal{A}$. Then $\Theta\,\Theta^*$ is a fractional left ideal in Θ. Thus $\Theta\,\Theta^* = \Theta\,\alpha$. $\Theta\,\Theta^*$ is 4-dimensional since Θ^* is 4-dimensional and $1 \in \Theta$. Thus $N\alpha \neq 0$. Now $\Theta\,\Theta^*$ is also a fractional right ideal in Θ^* and therefore

$\Theta\,\alpha\,\Theta^* \subset \Theta\,\alpha$. Since $1 \in \Theta$ we have $\alpha\,\Theta^* \subset \Theta\,\alpha$ and thus $\Theta^* \subset \alpha^{-1}\Theta\,\alpha$. But $\alpha^{-1}\Theta\,\alpha$ is an order and Θ^* is maximal. Therefore, $\Theta^* = \alpha^{-1}\Theta\,\alpha$.

Q.E.D.

(3.14) Theorem. There are $\dfrac{p^{r+1}-1}{p-1}$ right ideals in $\Theta = M_2(Z_p)$ of reduced norm p^r. They are generated by the quaternions ρ of the form

$$\begin{bmatrix} p^{r-t} & 0 \\ a & p^t \end{bmatrix}$$

where $a \in Z$, $0 \leq a < p^t$, $0 \leq t \leq r$.

Proof: Every submodule A of $Z_p \oplus Z_p$ has a triangular basis. That is, $A = [(x,y),(0,z)]$. If

$$\rho = \begin{bmatrix} x & 0 \\ y & z \end{bmatrix}$$

and $n(\rho\,\Theta) = p^r$, then $N\rho = xz = p^r$. Thus we may write $A = [(p^{r-t},y'),(0,p^t)]$. However, there is an $a \in Z$, $0 \leq a < p^t$ such that $a \equiv y' \bmod p^t$. Thus $A = [(p^{r-t},a),(0,p^t)]$. For every choice of t, $0 \leq t \leq r$, and for every choice of a mod p^t we obtain a distinct module A which corresponds to a right ideal of reduced norm p^r. Since there are p^t choices for a we see that there are $\sum_{t=0}^{r} p^t = \dfrac{p^{r+1}-1}{p-1}$ such

modules A and correspondingly $\frac{p^{r+1} - 1}{p - 1}$ distinct right ideals of reduced norm p^r.

Q.E.D.

(3.15) Corollary. There are $p^r + p^{r-1}$ primitive right ideals of Θ of reduced norm p^r.

Proof: Let

$$\rho = \begin{bmatrix} p^{r-t} & 0 \\ a & p^t \end{bmatrix} \quad , \; 0 \leq a < p^t \quad \text{be primitive.}$$

If $t \neq 0, r$, then a must be prime to p. There are $\varphi(p^t) = p^t - p^{t-1}$ such a's. If $t = 0$, there is only one ρ. If $t = r$, then ρ is primitive for every choice of a. Hence, there are

$1 + p^r + \sum_{t=1}^{r-1} (p^t - p^{t-1}) = p^r + p^{r-1}$ primitive ρ's which generate distinct right ideals of reduced norm p^r.

Q.E.D.

(3.16) Theorem. The primitive right ideals in Θ of reduced norm p^r are 2-dimensional mod p^r. Let

$$\rho = \begin{bmatrix} p^{r-t} & 0 \\ a & p^t \end{bmatrix} = p^{r-t}e_{11} + ae_{21} + p^t e_{22} \text{ be primitive.}$$

A basis for $\rho\,\Theta$ is $\rho\, e_{11} = p^{r-t}e_{11} + ae_{21}$, $\rho e_{12} = p^{r-t}e_{12} + ae_{22}$, $\rho\, e_{21} = p^{t}e_{21}$, $\rho\, e_{22} = p^{t}e_{22}$. If $t = 0$ or r, then $[\rho)$ is clearly 2-dimensional mod p^r. If $t \neq 0$, r, then a is prime to p. Thus $\rho\, e_{11}$, $\rho\, e_{12}$, $a\rho\, e_{21} - p^{t}\rho\, e_{11} = p^{r}e_{11}$, $a\rho\, e_{22} - p^{t}\rho\, e_{12} = p^{r}e_{22}$ is a basis for $[\rho)$. Clearly, $[\rho)$ is 2-dimensional mod p^r.

Q.E.D.

(3.17) Let M be the set of $p + 1$ quaternions

$$\begin{bmatrix} 1 & 0 \\ a & p \end{bmatrix}, \quad 0 \leq a < p, \text{ and } \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}.$$

Let M' be the set of transposes of the matrices in M. The elements of M (M') generate all of the $p + 1$ right (left) ideals of reduced norm p. If π is in M or M', then π is irreducible and $\pi^2 \equiv \pi \bmod p$.

(3.18) Theorem. The ideals $[\pi)$ are the maximal right ideals in Θ and every proper right ideal in Θ is contained in one of them. Moreover, if $\pi_1, \pi_2 \in M$ and $\pi_1 \neq \pi_2$, then $[\pi_1) \cap [\pi_2) = (p)$. (Similarly for the left ideals $(\pi]$, $\pi \in M'$)

Proof: $\Theta/p\Theta \simeq M_2(Z/pZ)$. By (3.12) the lattice of right ideals of $M_2(Z/pZ)$ is isomorphic to the lattice of submodules of $Z/pZ \oplus Z/pZ$.

Since Z/pZ is a field, the only proper submodules of $Z/pZ \oplus Z/pZ$ are 1-dimensional and are of the form $[(1,a)]$. $0 \leq a < p$ or $[(0,1)]$. These are the submodules corresponding to the ideals $[\pi)$ mod p. The intersection of any two distinct 1-dimensional submodules is easily seen to be 0-dimensional. Thus, if $\pi_1, \pi_2 \in M$ and $\pi_1 \not\equiv \pi_2$, then $[\pi_1) \cap [\pi_2) \equiv (0)$ mod p. But $p \in [\pi_1) \cap [\pi_2)$ and therefore $[\pi_1) \cap [\pi_2) = (p)$. If A is a proper right ideal in Θ, then A is contained in some $[\pi)$ mod p. Thus $A \subset [\pi) + (p) = [\pi)$. Therefore, the right ideals $[\pi)$ are maximal.

Q.E.D.

(3.19) Corollary. If A is a proper primitive right ideal in Θ, then there is a unique $\pi \in M$ such that $A \subset [\pi)$. Moreover, $[\pi) = A + (p)$.

(3.20) Theorem. If $\alpha, \beta \in \Theta$, then α and β belong to either the same maximal right ideal or the same maximal left ideal if and only if $N\alpha \equiv N\beta \equiv (\alpha,\beta) \equiv 0$ mod p.

Proof: If α and β lie in the same maximal ideal, then clearly $N\alpha \equiv N\beta \equiv (\alpha,\beta) \equiv 0$ mod p. Now suppose $N\alpha \equiv N\beta \equiv (\alpha,\beta) \equiv 0$ mod p. If one of α and β is not primitive, then obviously they both lie in some maximal right ideal. If both α and β are primitive, then $[\alpha)$ and $[\beta)$ are primitive. Thus $[\alpha) \equiv [\pi)$ mod p for some $\pi \in M$. Hence, $\pi \equiv \alpha\theta$ mod p for some unit θ. Let $\rho = \beta\theta$.

Then $N\pi \equiv N\rho \equiv (\pi, \rho) \equiv 0 \bmod p$ and, furthermore, π and ρ lie in the same ideal mod p if and only if α and β lie in the same ideal mod p. If $[\pi) \not\equiv [\rho)$, then $\Theta \equiv [\pi) \oplus [p)$ since both $[\pi)$ and $[\rho)$ are 2-dimensional mod p and $[\pi) \cap [\rho) \equiv (0)$. If $\pi\lambda \equiv \bar{\pi}\eta \bmod p$ for some $\lambda, \eta \in \Theta$, then $\pi\lambda \equiv \pi^2\lambda \equiv \pi\,\bar{\pi}\,\eta \equiv 0 \bmod p$. Thus $[\pi) \cap [\bar{\pi}) \equiv (0)$ and $\Theta \equiv [\pi) \oplus [\bar{\pi})$. Hence, there exist $\mu, \nu \in \Theta$ such that $\bar{\rho} \equiv \pi\mu + \bar{\pi}\nu$. Therefore, $\pi\bar{\rho} \equiv \pi^2\mu + \pi\bar{\pi}\nu \equiv \pi\mu \bmod p$. Adding $\rho\,\bar{\pi}$ to both sides we obtain $0 \equiv (\rho, \pi) \equiv \pi\bar{\rho} + \rho\,\bar{\pi} \equiv \pi\mu + \rho\,\bar{\pi}$. But since the sum $[\pi) + [p)$ is direct mod p, we must have $\pi\mu \equiv 0$. Therefore $\bar{\rho} \equiv \bar{\pi}\nu \bmod p$ and hence $[\bar{\rho}) \equiv [\bar{\pi})$. Therefore, $(\rho] \equiv (\pi]$.

Q.E.D.

(3.21) Lemma. Let S be a set, $A \subset S$, and R_1, R_2 be two symmetric, transitive, relations on S. If $A \times A \subset R_1 \cup R_2$, then $A \times A \subset R_1$ or $A \times A \subset R_2$.

Proof: Let a, b, c, d $\in$ A and suppose that $(a,b) \notin R_1$, $(c,d) \notin R_2$. Then $(a,b) \in R_2$, $(c,d) \in R_1$. If $(a,c) \in R_2$, then $(b,c) \in R_2$ and therefore neither (a,d) nor (b,d) is in R_2. Therefore, (a,d), (b,d) $\in R_1$ which contradicts the assumption that $(a,b) \notin R_1$. If $(a,c) \notin R_2$, then $(a,c) \in R_1$ and we reach a contradiction using the same argument with R_1 and R_2 interchanged. It follows that $A \times A \subset R_1$ or $A \times A \subset R_2$.

Q.E.D.

(3.22) Theorem. If A is a primitive 4-dimensional submodule of Θ and if $G_A = p^r F_A$, then there exist quaternions ρ and ρ' in Θ and a 4-dimensional submodule B of Θ such that

(i) $A = \rho B \rho'$,

(ii) $N(\rho \rho') = p^r$,

(iii) $G_B = F_B = F_A$.

Proof: If $r = 0$, the theorem is trivially true.

Suppose $r > 0$ and let A' be the set of all primitive quaternions in A. Let R_1 be the set of all (α, β) such that $\alpha, \beta \in A'$ and α and β lie in the same maximal right ideal. Let R_2 be the set of all (α, β) such that $\alpha, \beta \in A'$ and α and β lie in the same maximal left ideal. R_1, and similarly R_2, is an equivalence relation on Θ. For it is clearly reflexive and symmetric, and if (α, β), $(\beta, \gamma) \in R_1$, then $(\alpha, \gamma) \in R_1$ since β is primitive and therefore belongs to a unique maximal right ideal. Since $r > 0$, we have $N\alpha \equiv N\beta \equiv (\alpha, \beta) \equiv 0 \bmod p$ for all $\alpha, \beta \in A$. Hence, by (3.20), $A' \times A' \subset R_1 \cup R_2$ and thus, by (3.21), $A' \times A' \subset R_1$ or $A' \times A' \subset R_2$. Suppose $A' \times A' \subset R_1$ and let $\alpha \in A'$. Then every element $\beta \in A'$ belongs to the same maximal right ideal $[\pi)$ that α belongs to. Thus $A' \subset [\pi)$ and hence $A \subset [\pi)$. Therefore, $A = \pi \cdot A_1$ where $G_{A_1} = p^{r-1} F_{A_1}$. We proceed by induction and the theorem follows. Q.E.D.

(3.23) Corollary. If A is a 4-dimensional submodule of Θ, $G_A = p^r F_A$, and det F_A is a unit multiple of det F_Θ, then there is a right ideal R and a left ideal L such that $A = R \cdot L$.

Proof: By (3.22), $A = \rho B \rho'$ where $G_B = F_B = F_A$. Therefore, det G_B is a unit multiple of det F_Θ and thus $B = \Theta$. Hence, $A = \rho \Theta \rho' = [\rho)(\rho']$.

Q.E.D.

(3.24) Corollary. If A satisfies the conditions of (3.23) and if A is primitive, then the decomposition $A = R \cdot L$ is unique.

Proof: Suppose $A = R' \cdot L' = R \cdot L$. Then L and L' must be primitive. But then $L \cdot \Theta = \Theta$ and $L' \cdot \Theta = \Theta$ since the only primitive two-sided ideal in Θ is Θ. Therefore, $R = R \cdot \Theta = R(L \cdot \Theta) = A \cdot \Theta = R'(L' \cdot \Theta) = R'$ and, similarly, $L' = L$.

Q.E.D.

(3.25) Theorem. If R and L are primitive right ideals, then $A = R \cdot L$ is primitive and $N(A) = N(R) \cdot N(L)$.

Proof: If $A = R \cdot L = p^h \cdot B$, then $p^h \cdot \Theta \cdot B = \Theta \cdot R \cdot L = L$ and thus $h = 0$. Also, $G_A = n(R) \cdot n(L) F_\Theta$. Hence, $F_A = F_\Theta$ and det $G_A = N(A)^2 \cdot$ det F_Θ $= n(R)^4 n(L)^4 \cdot$ det F_Θ. Therefore, $N(A) = n(R)^2 n(L)^2 = N(R) \cdot N(L)$.

Q.E.D.

CHAPTER IV

THE GLOBAL CASE

Let $\mathcal{A}$ be a quaternion algebra over $\mathbb{Q}$ with basis ρ_0, ρ_1, ρ_2, ρ_3. We define the local algebra $\mathcal{A}_p$ over $\mathbb{Q}_p$ in the following manner. Let $\mathcal{A}_p$ be a 4-dimensional vector space over $\mathbb{Q}_p$ with the same basis ρ_0, ρ_1, ρ_2, ρ_3. Let the ρ_k have the same multiplication table as they did in $\mathcal{A}$ and extend by linearity to a multiplication on all of $\mathcal{A}_p$. We can obviously consider $\mathcal{A}$ as a subset of $\mathcal{A}_p$ with the same multiplication as before. If $A = \sum_0^3 Z\alpha_i$ is a Z-module in $\mathcal{A}$, we let $A_p = Z_p \cdot A = \sum_0^3 Z_p \alpha_i$. If A is a 4-dimensional Z-module, then the rational transformation taking the ρ basis onto the α basis is also a p-adic transformation and has non-zero determinant. Thus, A_p is a 4-dimensional Z_p-module and $G_{A_p} = G_A$. If $\Theta = \Theta(f)$ is a principal Z-order in $\mathcal{A}$, then clearly Θ_p is a principal Z_p-order in $\mathcal{A}_p$. We call $d = -4 \cdot \det f$ the <u>discriminant</u> of f (and of $\Theta(f)$). It can be seen from (3.4) and (3.13) or from [6;287] that a necessary and sufficient condition that Θ_p be maximal is that $p^2 \nmid d$ and if $p \mid d$, then $c_p(f) = -1$. Primes which satisfy this last condition will be called <u>good</u>; the other primes (of which there are only finitely many)

will be called bad.

The Z-modules in Θ will be denoted by A, B, etc., while the Z_p-modules in Θ_p will be denoted by $A^{(p)}$, $B^{(p)}$, etc., or by A_p, B_p, etc. We call $A^{(p)c} = A^{(p)} \cap \Theta$ the contraction of $A^{(p)}$ to Θ.

We need to know the rules for going back and forth between the global and local algebras.

(4.1) Lemma. Let A be a 4-dimensional submodule of Θ. Then $A_p^c = \{\alpha \in \Theta \mid s\alpha \in A \text{ for some integer } s \text{ prime to } p\}$.

Proof: If $\alpha \in \Theta$ and $s\alpha \in A$ for some integer s prime to p, then $\alpha \in A_p$ since s is a p-adic unit and hence $\alpha \in A_p \cap \Theta = A_p^c$.

Now let $A = [\alpha_0, \alpha_1, \alpha_2, \alpha_3]$. If $\alpha \in \Theta$, then there exist unique $x_i \in \mathbb{Q}$ such that $\alpha = \Sigma x_i \alpha_i$. But if α is also in A_p, then each $x_i \in Z_p$. Thus, there is an integer s, prime to p, such that $sx_i \in Z$ for each i and therefore $s\alpha \in A$.

Q.E.D.

(4.2) Lemma. If A and B are 4-dimensional submodules of Θ and $A^{(p)}$ and $B^{(p)}$ are 4-dimensional submodules of Θ_p, then

(i) $A \subset A_p^c$, $A^{(p)} \supset (A^{(p)c})_p$

(ii) $A_p = (A_p^c)_p$, $A^{(p)c} = (A^{(p)c})_p^c$

(iii) $(A \cdot B)_p = A_p \cdot B_p$, $(A^{(p)} \cap B^{(p)})^c = A^{(p)c} \cap B^{(p)c}$

(iv) $(A \cap B)_p \subset A_p \cap B_p$, $(A^{(p)} \cdot B^{(p)})^c \supset A^{(p)c} \cdot B^{(p)c}$

(v) $A = A_p^c$ if and only if $N(A)$ or $n(A)$ is a power of p.

(vi) $A^{(p)} = (A^{(p)c})_p$ if and only if there exists a Z_p basis $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ for $A^{(p)}$ with each $\alpha_i \in \Theta$.

(vii) $A_p = \Theta_p$ if and only if $p \nmid N(A)$.

(viii) $$N(A) = \prod_p N(A_p) = \prod_{p|N(A)} N(A_p), \quad n(A) = \prod_p n(A_p) = \prod_{p|N(A)} n(A_p)$$

$$l(A) = \prod_p l(A_p) = \prod_{p|N(A)} l(A_p).$$

Proof: (i), (iii), (iv), (vii), and (viii) are trivial.

(ii) By (i), $A_p \supset (A_p^c)_p$ and $A \subset A_p^c$. Thus, $A_p \subset (A_p^c)_p \subset A_p$. Therefore, $A_p = (A_p^c)_p$. Again by (i), $A^{(p)c} \subset (A^{(p)c})_p^c$ and $(A^{(p)c})_p \subset A^{(p)}$. Thus, $A^{(p)c} \subset (A^{(p)c})_p^c \subset A^{(p)c}$. Therefore, $A^{(p)c} = (A^{(p)c})_p^c$.

(v) Let T be the transformation taking Θ onto A. By (2.6) and (2.7), we know $N(A) = |\det T|$, $n(A) \mid N(A)$, and $T \cdot S = \pm n(A) \cdot I$ for some primitive matrix S. Taking determinants gives $N(A) \cdot \det S = n(A)^4$. Thus $p \mid N(A)$ if and only if $p \mid n(A)$. Suppose $A = A_p^c$. We know

that $n(A)$ is the least positive integer h such that $h\cdot\Theta \subset A$. If $n(A) = p^r s$ with s prime to p, then $sp^r\cdot\Theta \subset A$. But by (4.1) and by the assumption that $A = A_p^c$, this means $p^r\cdot\Theta \subset A$. Thus, $s = 1$ and $n(A)$ and $N(A)$ are powers of p. Now suppose $n(A) = p^r$ and $A = [\alpha_0, \alpha_1, \alpha_2, \alpha_3]$. If $\alpha \in \Theta$, then $\alpha = \frac{1}{p^r}\cdot\alpha'$ for some $\alpha' = \Sigma x_i\alpha_i \in A$, since $p^r\Theta \subset A$. Thus, if $s\alpha \in A$ for some s prime to p, then $p^{-r}\cdot s\alpha' = \Sigma p^{-r}sx_i\alpha_i \in A$. Therefore, $p^r \mid x_i$ for each i and $\alpha \in A$. In view of (4.1), we see that $A = A_p^c$.

(vi) Suppose $A^{(p)} = Z_p[\alpha_0, \alpha_1, \alpha_2, \alpha_3]$ with $\alpha_i \in \Theta$. Let $A = Z[\alpha_0, \alpha_1, \alpha_2, \alpha_3]$. Then $A \subset A^{(p)c} \subset A^{(p)}$. Hence, $A^{(p)} = A_p \subset (A^{(p)c})_p \subset A^{(p)}$ and therefore $A^{(p)} = (A^{(p)c})_p$. Now suppose $A^{(p)} = (A^{(p)c})_p$. Since $A^{(p)c} \subset \Theta$ and is a Z-module, then $A^{(p)c} = Z[\alpha_0, \alpha_1, \alpha_2, \alpha_3]$ for some $\alpha_i \in \Theta$. Thus $A^{(p)} = (A^{(p)c})_p = Z_p[\alpha_0, \alpha_1, \alpha_2, \alpha_3]$ with $\alpha_i \in \Theta$.

Q.E.D.

(4.3) Lemma. If $A^{(p)}$ is a 4-dimensional Z_p-module in Θ_p, then $A^{(p)}$ has a basis $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ with $\alpha_i \in \Theta$ and consequently $A^{(p)} = (A^{(p)c})_p$,

$N(A^{(p)}) = N(A^{(p)c})$, $n(A^{(p)}) = n(A^{(p)c})$, and $l(A^{(p)}) = l(A^{(p)c})$.

Proof: If $A^{(p)}$ is 4-dimensional, then $n(A^{(p)}) = p^r$ for some $r \geq 0$. If $r = 0$, then $A^{(p)} = \Theta_p$ and the theorem is true. If $r > 0$, let $A^{(p)} = Z_p[\alpha_0, \alpha_1, \alpha_2, \alpha_3]$. There exist $\alpha_i' \in \Theta$ such that $\alpha_i' \equiv \alpha_i \pmod{p^r}$ and thus, $\alpha_i' = \alpha_i + p^r\gamma_i$ for some $\gamma_i \in \Theta_p$. Let $A = Z[\alpha_0', \alpha_1', \alpha_2', \alpha_3'] + p^r\Theta = Z[\beta_0, \beta_1, \beta_2, \beta_3]$. Then $A_p = Z_p[\alpha_0', \alpha_1', \alpha_2', \alpha_3'] + p^r\Theta_p = Z_p[\beta_0, \beta_1, \beta_2, \beta_3]$. Clearly, $A_p \subset A(p)$, and since $p^r\gamma_i \in A_p$ for each i, we have $\alpha_i \in A_p$. Thus $A^{(p)} = A_p = Z_p[\beta_0, \beta_1, \beta_2, \beta_3]$ with $\beta_i \in \Theta$. The rest of the theorem follows easily.

Q.E.D.

(4.4) Theorem. If $A = [\alpha_0, \alpha_1, \alpha_2, \alpha_3]$ is a 4-dimensional submodule of Θ, then $A = \bigcap_{p \mid N(A)} A_p^c$. Moreover, if $A^{(p)}$ is a 4-dimensional Θ_p-module for each rational prime p and if $A = \bigcap_p A^{(p)c}$, then $A_p = A^{(p)}$ for each prime p.

Proof: By (4.2.i), we have $A \subset \bigcap_p A_p^c$. If $\xi \in \bigcap_p A_p^c$, then $\xi \in \Theta$, and thus there exist unique $x_i \in Q$ such that $\xi = \Sigma x_i \alpha_i$. But then each $x_i \in Z_p$ for every prime p. Thus each $x_i \in Z$, $\xi \in A$, and therefore $A = \bigcap_p A_p^c$. Now if $p \nmid N(A)$, then $A_p = \Theta_p$, and hence $A_p^c = \Theta$. Therefore, $A = \bigcap_{p|N(A)} A_p^c$. Now suppose $A = \bigcap_p A^{(p)c}$ with each $A^{(p)}$ 4-dimensional. Then $A \subset A^{(p)c}$ for each p, and hence $A_p \subset (A^{(p)c})_p = A^{(p)}$ for each p. Thus $n(A^{(p)}) \mid n(A_p)$ for each p. Let $h = \prod_p n(A^{(p)}) = \prod_p n(A^{(p)c})$ and $h_p = \frac{h}{n(A^{(p)})}$. We see that $(h_p, p) = 1$ and that $h_p \cdot \Theta \subset A^{(q)c}$ for every prime $q \neq p$. In particular, we have $h_p \cdot A^{(p)c} \subset A^{(q)c}$ for every $q \neq p$. However, $h_p \cdot A^{(p)c} \subset A^{(p)c}$ and therefore $h_p \cdot A^{(p)c} \subset \bigcap_q A^{(q)c} = A$. Thus, $h_p \cdot A^{(p)} = h_p \cdot (A^{(p)c})_p \subset A_p$. But h_p is a unit in Z_p and thus $A^{(p)} \subset A_p \subset A^{(p)}$. Therefore, $A_p = A^{(p)}$.

Q.E.D.

(4.5) Corollary. If $A^{(p)}$ is a 4-dimensional submodule of Θ_p for each prime p and if $A^{(p)} = \Theta_p$ for all but a finite number of primes,

then $A = \bigcap_p A^{(p)c}$ is a 4-dimensional submodule of Θ. Furthermore,

$N(A) = \prod_p N(A^{(p)})$, $n(A) = \prod_p n(A^{(p)})$, and $l(A) = \prod_p l(A^{(p)})$.

(4.6) Theorem. If R is a primitive right ideal in Θ such that $n(R)$ is divisible by good primes only, then $N(R) = n(R)^2$, $G_R = n(R)\cdot F_R$, and there exists a primitive $\xi \in R$ such that $R = [n(R), \xi)$ and the g.c.d.$\{n(R), \frac{N\xi}{n(R)}\} = 1$.

Proof: Since R is primitive, each R_p is primitive. By (2.9), we have $N(R_p) = n(R_p)^2$ and thus $G_{R_p} = n(R_p)\cdot F_{\Theta_p}$. Thus, $N(R) = \prod N(R_p) = \prod n(R_p)^2 = n(R)^2$. Now $G_R = mF_R$ for some positive integer m. But $G_R = G_{R_p}$ for each p. Thus, $n(R_p) \mid m$ for each p and therefore $m = n(R)\cdot m'$. However, m' is a unit in Z_p for each p. Therefore, $m' = 1$ and $G_R = n(R)\cdot F_R$. Now let $n(R) = p_1^{r_1} \cdots p_u^{r_u}$ and $R_{p_i} = \alpha_i \cdot \Theta_{p_i}$ with $N\alpha_i = p_i^{r_i}$ so that $R = \bigcap_{i=1}^{u} R^c_{p_i}$. For each i there exists $\xi_i \in R^c_{p_i}$ such that $\alpha_i \equiv \xi_i \bmod p_i^{2r_i}$. Let $h = n(R)^2$ and $h_i = h\cdot p_i^{-2r_i}$. Then h_i is prime to p_i so there exists $k_i \in Z$

such that $h_i k_i \equiv 1 \bmod p_i^{2r_i}$. Finally, let $\xi = \Sigma h_i k_i \xi_i$, and consider the ideal $[n(R), \xi)$ in Θ. If $p \nmid n(R)$, then $[n(R), \xi)_p = \Theta_p$. If $p = p_i$ divides $n(R)$, then $\xi \equiv \xi_i \equiv \alpha_i \bmod p_i^{2r_i}$. Thus, $[n(R), \xi)_{p_i} = [p_i^{r_i}, \alpha_i)_{p_i} = \alpha_i \Theta_{p_i} = R_{p_i}$. Therefore, $R = [n(R), \xi)$. Moreover, $N\xi \equiv N\alpha_i \equiv p_i^{r_i} \bmod p_i^{2r_i}$ and therefore the g.c.d.$\{n(R), \frac{N\xi}{n(R)}\} = 1$. From the construction of ξ, it is clear that if $p \mid n(R)$, then $p \nmid \xi$ in Θ. Thus, if $\xi = s\xi'$ with $s \in Z$ and ξ' primitive, then s is prime to $n(R)$ and there exist integers a and b such that $as + b \cdot n(R) = 1$. Hence, $\xi' = as\xi' + b \cdot n(R)\xi' = a\xi + b \cdot n(R)\xi' \in [n(R), \xi)$. Since a is prime to $n(R)$, it is clear that $[n(R), \xi') = [n(R), \xi)$. Furthermore, $N\xi' = a^2 N\xi + ab \cdot n(R) \cdot (\xi, \xi') + b^2 \cdot n(R)^2 N\xi'$. Since $n(R) \mid (\xi, \xi')$ we have the g.c.d.$\{n(R), \frac{N\xi'}{n(R)}\} = 1$.

Q.E.D.

(4.7) Theorem. Let R be a primitive right ideal in $\Theta(f)$ such that $n(R)$ is divisible by good primes only. If $n(R) = m_1 m_2$ where m_1 is the largest factor of m divisible only by primes for which $c_p(f) = -1$, then the two-sided ideal $I = \Theta \cdot R$ is the ideal $\bigcap_{p \mid m_1} R^c_p$ and $n(I) = m_1$.

Proof: If $c_p(f) = +1$, then $I_p = \Theta_p \cdot R_p = \Theta_p$ since R_p is primitive. If $c_p(f) = -1$, then $I_p = \Theta_p \cdot R_p = R_p$ since ideals are two-sided in this case. Therefore, $I = \bigcap_{p|m_1} R_p^c$ and $n(I) = m_1$.

Q.E.D.

(4.8) Theorem. The two-sided ideals in $\Theta(f)$ whose reduced norms are divisible by good primes only commute. If I is a primitive such ideal, then $I^2 = n(I) \cdot \Theta$.

Proof: The theorem is true if it is true for primitive two-sided ideals. Let I and J be primitive two-sided ideals whose reduced norms satisfy the conditions of the theorem. If $c_p(f) = +1$, then $I_p = J_p = \Theta_p$ since I_p and J_p are primitive. If $c_p(f) = -1$, then $(IJ)_p = I_p \cdot J_p = J_p \cdot I_p = (J \cdot I)_p$. Thus IJ = JI. Again, if I is primitive, the only primes p that divide n(I) are those for which $c_p(f) = -1$. If $p \mid n(I)$, then I_p is a proper primitive ideal of Θ_p and thus is the maximal ideal (π). But $(\pi)^2 = (p)$. Hence, $n(I_p) = p$ and $(I_p)^2 = p\,\Theta_p$. Therefore, $I^2 = \bigcap I_p^c = \bigcap_{p|n(I)} p\,\Theta = (\prod_{p|n(I)} p) \cdot \Theta = n(I) \cdot \Theta$.

Q.E.D.

(4.9) Theorem. Let A be a primitive, 4-dimensional submodule of Θ with $G_A = mF_A$ and $\det F_A = \det F_\Theta$. If m is divisible by good primes only, then there exists a unique triplet of integers (a,b,c) and unique right, two-sided, and left ideals R, I, and L, respectively, such that

(i) $A = RIL$

(ii) $m = abc$ with b the largest factor of m divisible only by primes for which $c_p(f) = -1$

(iii) $n(R) = a$, $n(I) = b$, $n(L) = c$.

Proof: If $p \nmid m$, then $\det G_A$ is a p-adic unit times $\det F_{\Theta_p}$ and hence $A_p = \Theta_p$. If $p \mid m$, then $G_{A_p} = p^r m' F_{A_p}$ where m' is a p-adic unit. Thus, $\det m'F_{A_p}$ is a unit multiple of $\det F_{\Theta_p}$. Hence by (3.8) if $c_p(f) = -1$, then A_p is a two-sided ideal of Θ_p, and by (3.23) if $c_p(f) = +1$, then A_p is uniquely expressible as a product $R^{(p)} \cdot L^{(p)}$ of a right and left ideal in Θ_p. Now let b be the largest factor of m for which $c_p(f) = -1$ and let $m' = \frac{m}{b}$. Let $I = \bigcap_{p|b} A^c_p$, $R = \bigcap_{p|m'} R^{(p)c}$, $L = \bigcap_{p|m'} L^{(p)c}$, and $B = R \cdot I \cdot L$. Then $B_p = R_p \cdot I_p \cdot L_p$. Thus, $B_p = A_p$ if

$p \mid b$, $B_p = R^{(p)} \cdot I_p \cdot L^{(p)} = R^{(p)} L^{(p)} = A_p$ if $p \mid m'$, and

$B_p = \Theta_p = A_p$ if $p \nmid m$. Thus, $A = B = R \cdot I \cdot L$. Clearly, $n(I) = b$.

Let $n(R) = a$, $n(L) = c$. If $p \mid m'$ we know that $G_{A_p} = n(R_p) \cdot n(L_p) F_{\Theta_p}$

and if $p \mid b$ we know that $G_{A_p} = n(A_p) \cdot F_{\Theta_p}$. Therefore,

$$m = \prod_{p \mid m'} n(R_p) \cdot \prod_{p \mid b} n(A_p) \cdot \prod_{p \mid m'} n(L_p) = abc.$$

Q.E.D.

Let $\Theta = Z[\omega_0, \omega_1, \omega_2, \omega_3]$ be a principal order in $\mathcal{A}$ and let $\Omega = (\omega_0, \omega_1, \omega_2, \omega_3)$. For $\alpha \in \mathcal{A}$ there exist unique matrices $\varphi(\alpha)$, $\psi(\alpha) \in M_4(Q)$ such that $\alpha \Omega = \Omega \cdot \varphi(\alpha)$ and $\Omega \alpha = \Omega \psi(\alpha)$. It is easily shown that $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$, $\varphi(\alpha \beta) = \varphi(\alpha) \cdot \varphi(\beta)$, and that $\psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$, $\psi(\alpha \beta) = \psi(\beta) \cdot \psi(\alpha)$. Thus, φ is a Q-homomorphism and ψ is a Q-anti-homomorphism of $\mathcal{A}$ into $M_4(Q)$. $\mathcal{A}$ is simple and therefore each of $\ker \varphi$ and $\ker \psi$ is either 0 or $\mathcal{A}$. But $1 \in \mathcal{A}$ and hence $\varphi(1) = \psi(1) = I_4 \neq 0$. Thus $\ker \varphi = \ker \psi = 0$ and therefore φ and ψ are monomorphisms. Now $\alpha \Omega \beta = \alpha(\Omega \beta) = (\alpha \Omega)\psi(\beta) = \Omega \varphi(\alpha) \cdot \psi(\beta)$ on one hand, and on the other hand, $\alpha \Omega \beta = (\alpha \Omega)\beta = \Omega \varphi(\alpha)\beta = (\Omega \beta)\varphi(\alpha) = \Omega \psi(\beta) \cdot \varphi(\alpha)$. Therefore, $\varphi(\alpha) \cdot \psi(\beta) = \psi(\beta) \cdot \varphi(\alpha)$ for every $\alpha, \beta \in \mathcal{A}$. If we restrict φ and ψ to Θ, they they are

monomorphisms from Θ into $M_4(Z)$. We can now apply (4.9) to derive an interesting result.

(4.10) Theorem. Let $T \in M_4(z)$ be a primitive matrix such that $T'T = mI$ where m is an odd positive integer. Then there is a unique pair of integers (m_1,m_2) and there exist matrices

$$M = \begin{bmatrix} x_0 & -x_1 & -x_2 & -x_3 \\ x_1 & x_0 & -x_3 & x_2 \\ x_2 & x_3 & x_0 & -x_1 \\ x_3 & -x_2 & x_1 & x_0 \end{bmatrix}, \quad N = \begin{bmatrix} y_0 & -y_1 & -y_2 & -y_3 \\ y_1 & y_0 & y_3 & -y_2 \\ y_2 & -y_3 & y_0 & y_1 \\ y_3 & y_2 & -y_1 & y_0 \end{bmatrix}$$ with

$x_0^2 + x_1^2 + x_2^2 + x_3^2 = m_1$, $y_0^2 + y_1^2 + y_2^2 + y_3^2 = m_2$, $m = m_1m_2$, and a unit-modular matrix $U \in M_4(Z)$ such that $T = MNU = NMU$.

Proof: Let $f = x^2 + y^2 + z^2$. Then $\Theta(f)$ is the ring of Lipschitz quaternions with the usual basis 1, i, j, k. The norm form for this basis is $F_\Theta = x_0^2 + x_1^2 + x_2^2 + x_3^2$. The prime 2 is the only bad prime in this order and $c_p(f) = +1$ for odd primes. It is well known that the ideals of odd norm are all principal. Now let $\Omega = (1,i,j,k)$ and A be the submodule whose basis is ΩT. Then A is primitive and $G_A = m(x_0^2 + x_1^2 + x_2^2 + x_3^2)$. Since m is odd, $C_p(f) = +1$ for every prime dividing m. Thus, by (4.9) there exists a unique pair (m_1,m_2) of integers and unique right and left ideals R and L, respectively, such

that $A = R \cdot L$, $n(R) = m_1$, $n(L) = m_2$, and $m = m_1 m_2$. But m_1 and m_2 are odd and thus $R = [\xi)$, $L = (\eta]$ for some $\xi = x_0 + x_1 i + x_2 j + x_3 k$ and $\eta = y_0 + y_1 i + y_2 j + y_3 k$. Moreover, $x_0^2 + x_1^2 + x_2^2 + x_3^2 = N\xi = n(R) = m_1$, $y_0^2 + y_1^2 + y_2^2 + y_3^2 = N\eta = n(L) = m_2$, and, by direct computation, $\varphi(\xi) = M$, $\psi(\eta) = N$. It is easily seen that $\xi\ \Omega\ \eta$ is a basis for $[\xi) \cdot (\eta] = A$. Thus, there is a unit-modular matrix $U \in M_4(Z)$ such that $\Omega T = \Omega\ \varphi(\xi)\psi(\eta)U = \Omega\ \psi(\eta)\varphi(\xi)U$. Therefore, $T = MNU = NMU$.

Q.E.D.

Notice that ξ and η can be written as the product of irreducible quaternions of prime norm. That is $\xi = \pi_1 \cdot \pi_2 \cdots \pi_h$ and $\eta = \pi_1' \pi_2' \cdots \pi_k'$ with $N\pi_i$ and $N\pi_i'$ primes for each i. Thus, $M = \varphi(\xi) = \varphi(\pi_1) \cdot \varphi(\pi_2) \cdots \varphi(\pi_h)$ and $N = \psi(\eta) = \psi(\pi_k') \cdots \psi(\pi_2') \cdot \psi(\pi_1')$ where $\varphi(\pi_i)$ has the same form as M and $\psi(\pi_j')$ has the same form as N.

Other applications of (4.9) and the theory developed in this thesis should be possible. One such is the generalization of (4.10) to

(4.11) Conjecture. If F is a norm form of some principal order Θ, and if $T \in M_4(Z)$ is a primitive matrix such that $F^T = mF$ and m is the product of good primes, then there exist matrices M_i, N_j, $P_k \in M_4(Z)$, $i = 1, \ldots, r$, $j = 1, \ldots, s$, $k = 1, \ldots, t$, and a unit-modular matrix $U \in M_4(Z)$ such that $T = (N_1 N_2 \cdots N_r) \cdot (M_1 \cdots M_s) \cdot (P_1 \cdots P_t)$, $\det N_i$, $\det M_j$, $\det P_k$ are primes, and $N_i M_j = M_j N_i$, $N_i P_j = P_j N_i$, $M_i P_j = P_j M_i$, $P_i P_j = P_j P_i$.

SELECTED BIBLIOGRAPHY

1. Artin, Emil. " Zur Arithmetik hyperkomplexen Zahlen," Abhandlung Mathematisches Seminar, Universität Hamburg, 5(1928), 261-289.

2. Hasse, Helmut. " Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme." Mathematische Annalen, V. 104(1930-1931), Verlag von Julius Springer, Berlin, 495.

3. Jacobson, Nathan. The Theory of Rings. American Mathematical Society, Mathematical Surveys, II, New York, 1943.

4. Mann, Henry B. Introduction to Algebraic Number Theory. The Ohio State University Press, Columbus, 1955.

5. O'Meara, O.T. Introduction to Quadratic Forms. Springer-Verlag, Berlin, 1963.

6. Pall, Gordon. " On Generalized Quaternions," Transactions of the American Mathematical Society, LIX(1946), 280-332.

7. Van der Blij, F. and Springer, T. A. " The Arithmetic of Octaves and of the Group G_2," Indagationes Mathematicae, (1959), 406-418.

AUTOBIOGRAPHY

Charles Carter Waid, son of Dr. and Mrs. Guy N. Waid, was born February 27, 1939, in Okeene, Oklahoma. He graduated from Carlsbad High School in Carlsbad, New Mexico, in June, 1957. He entered New Mexico Institute of Mining and Technology in June, 1957, and received his Bachelor of Science degree in mathematics in June, 1961. He then taught for one year at East Junior High School, Roswell, New Mexico.

He enrolled in the Graduate School of Louisiana State University in September, 1962, and received a Master of Science degree in mathematics in June, 1964.

From September, 1962, through August, 1966, he held a Graduate Teaching Assistantship. In September, 1966, he was appointed Instructor of Mathematics. In March, 1963, he was married to Margaret Yvonne Cowsar who received her Master of Science degree in mathematics from Louisiana State University in August, 1963. They have two sons, James Bryan and Gordon Chester, who were born in April, 1964, and November, 1966, respectively.

He is presently a candidate for the degree of Doctor of Philosophy in Mathematics.

EXAMINATION AND THESIS REPORT

Candidate: Charles Carter Waid

Major Field: Mathematics

Title of Thesis: MODULES OF QUATERNIONS AND THEIR RELATED QUADRATIC FORMS

Approved:

Gordon Pall
Major Professor and Chairman

Max Goodrich
Dean of the Graduate School

EXAMINING COMMITTEE:

Gordon Pall

L. J. Wade

J. Leslie

J. Darroch

H. S. Butts

Date of Examination:

July 14, 1967